

# HACKER DALAM PERSPEKTIF HUKUM INDONESIA

Bambang Hartono

Fakultas Hukum UBL  
Jl. Za Pagar Alam No 26 Labuhan Ratu, Bandar Lampung 35142  
email: bambanghartono@rocketmail.com

## Abstract

*Hacker is a Cyber Crimes, often occur but until now there has been no legal basis of the most powerful to handle the cases, even the development of cybercrime in the world is getting fierce. In addition to using advanced tools, modes of cybercrime is also quite neat. This is so great crimes can be devastating even internationally. Cybercrime is quite complicated dynamics. Therefore, do not recognize national boundaries and regions. In addition, the time the crime was difficult to determine. Cyber Crime is a phenomenon full rank candidates for the biggest crime in the future.*

**Keywords :** Hackers, Cyber Crime. Legal Basis

## Abstrak

*Hacker merupakan Cyber Crimes, kerap terjadi namun hingga sekarang belum ada pilar hukum paling ampuh untuk menangani kasus-kasusnya, bahkan perkembangan kejahatan di dunia cyber semakin dahsyat. Selain menggunakan piranti canggih, modus kejahatan cyber juga tergolong rapi. Begitu hebatnya kejahatan ini bahkan dapat meresahkan dunia internasional. Dinamika cybercrime memang cukup rumit. Sebab, tidak mengenal batas negara dan wilayah. Selain itu, waktu kejahatannya pun sulit ditentukan. Lengkap sudah fenomena Cyber Crime untuk menduduki peringkat calon kejahatan terbesar di masa mendatang.*

**Kata Kunci:** Hacker, Cyber Crime. Legal Basis

### A. Pendahuluan

Kemajuan ilmu dan teknologi ikut membuat jenis dan bentuk kejahatan semakin canggih, ragam, rumit, dan sulit untuk dipecahkan. Tak hanya itu, kejahatan yang terjadi juga makin mengabaikan batas-batas negara. Karena itu, usaha memerangi kejahatan tersebut hanya bisa dilakukan secara bersama (antar negara), yang sejauh ini harus diakui masih sangat terbatas dan membutuhkan perbaikan maupun peningkatan.

Perkembangan ilmu pengetahuan dan teknologi (iptek) yang cukup pesat sekarang ini sudah menjadi realita sehari-hari bahkan merupakan tuntutan masyarakat yang tidak dapat ditawar lagi. Tujuan utama perkembangan iptek adalah perubahan kehidupan masa depan manusia yang lebih baik, mudah, murah, cepat dan aman. Perkembangan iptek, terutama teknologi informasi (information technology) seperti internet sangat

menunjang setiap orang mencapai tujuan hidupnya dalam waktu singkat, baik legal maupun illegal dengan menghalalkan segala cara karena ingin memperoleh keuntungan secara “potong kompas”. Dampak buruk dari perkembangan “Dunia Maya” ini tidak dapat dihindarkan dalam kehidupan masyarakat moderen saat ini dan masa depan. **Barda Nawawi Arief**, menyatakan bahwa Beredarnya foto hubungan seksual seorang siswi di Sampit beberapa waktu yang lalu, yang direkam dengan kamera digital dan disebarluaskan melalui MMS (*multy media message*), merupakan salah satu contoh penyalahgunaan teknologi maju. Akhir-akhir ini muncul kasus video mesum mirip Ariel dan Luna Maya yang mendapat berbagai tanggapan memprihatinkan dari berbagai kalangan masyarakat dan pejabat karena mempunyai dampak dan reaksi/respons sangat luas.<sup>1</sup>

Kemajuan teknologi informasi yang serba

1 Barda Nawawi Arief, 2011...*Pornografi, Cyberporn dan Porno Aksi*, Semarang, Badan Penerbit Universitas Diponegoro, hlm. 13.

digital membawa orang ke dunia bisnis yang revolusioner (digital revolution era) karena dirasakan lebih mudah, murah, praktis dan dinamis berkomunikasi dan memperoleh informasi. Di sisi lain, berkembangnya teknologi informasi menimbulkan pula sisi rawan yang gelap sampai tahap mencemaskan dengan kekhawatiran pada perkembangan tindak pidana di bidang teknologi informasi yang berhubungan dengan “**cybercrime**” atau kejahatan mayantara.<sup>2</sup>

Masalah kejahatan mayantara dewasa ini sepatutnya mendapat perhatian semua pihak secara seksama pada perkembangan teknologi informasi masa depan, karena kejahatan ini termasuk salah satu *extra ordinary crime* (kejahatan luar biasa) bahkan dirasakan pula sebagai *serious crime* (kejahatan serius) dan *transnational crime* (kejahatan antar negara) yang selalu mengancam kehidupan warga masyarakat, bangsa dan negara berdaulat. Tindak pidana atau kejahatan ini adalah sisi paling buruk di dalam kehidupan moderen dari masyarakat informasi akibat kemajuan pesat teknologi dengan meningkatnya peristiwa kejahatan komputer, pornografi, terorisme digital, “perang” informasi sampah, bias informasi, hacker, cracker dan sebagainya.

Peristiwa kejahatan mayantara yang pernah menimpa situs Mabes TNI, Badan Pengkajian dan Penerapan Teknologi (BPPT), Mabes Polri dan Departemen Luar Negeri Republik Indonesia merupakan sisi gelap dari kejahatan teknologi informasi yang memanfaatkan kecanggihan internet. Begitu juga situs Microsoft, NASA dan

Pentagon tidak luput pula dari para hacker nakal untuk mengacaukan sistem informasi dan data yang dimiliki oleh negara adidaya, Amerika Serikat. Ketegangan antara Cina dengan Amerika Serikat sempat pula mengarah pada perang hacker karena mengubah situs FBI menjadi wajah pilot Cina yang tewas dalam suatu insiden di Laut Cina Selatan dengan pesawat pengintai Amerika yang berada di wilayah udara Cina.<sup>3</sup>

Semua peristiwa di atas adalah beberapa contoh disalahgunakannya kemajuan teknologi informasi untuk tujuan buruk yang dapat merugikan pihak lain dalam tatanan dunia semakin maju dalam globalisasi ekonomi. Inilah sebenarnya salah satu sisi paling buruk yang tidak dapat dihindarkan dan disembunyikan dari kemajuan teknologi informasi dewasa ini sebagaimana pernah diramalkan oleh John Naisbitt dan Patricia Aburdene<sup>4</sup> bakal ada perubahan dunia menjadi perkampungan global (global village) dengan pola satu sistem perekonomian atau single economy system, yaitu sistem ekonomi kapitalis. Sistem ekonomi demikian dapat menyebabkan orang menghalalkan segala cara, terutama pada saat berlakunya pasar bebas (free market) untuk mencapai tujuannya dengan menggunakan sarana teknologi canggih.

Masalah ini segera menjadi pusat perhatian dari masyarakat internasional. Pada *International Information Industry Congress (IIC) 2000 Millenium* di Quebec, Kanada, tanggal 19 September 2000 merumuskan perlunya kewaspadaan terhadap perkembangan *cybercrimes* yang dapat merusak sistem dan data vital teknologi perusahaan dalam

- 
- 2 Lihat Barda Nawawi Arief, 2001, “*Kebijakan Kriminalisasi dan Masalah Yurisdiksi Tindak Pidana Mayantara*”, Seminar Nasional RUU Teknologi Informasi (Cyber-Law) “*Pemberdayaan Teknologi Informasi dalam Masyarakat Informasi*”, Kerjasama Dirjen Postel DEPHUB dengan UNDIP, Gedung Ghradhika Bhakti Praja, Semarang,
  - 3 Baru-baru ini Kepolisian telah berhasil mengamankan seorang hacker yang meretas situs presiden SBY yang beralamatkan di [www.president.sby.info](http://www.president.sby.info). Situs Presiden SBY tersebut di-hack oleh pelaku yang meninggalkan identitas sebagai Jember Hacker. “Sudah diamankan oleh Bareskrim Mabes Polri beberapa hari yang lalu.” ujar AKBP Jayadi, Kapolres Jember, Selasa 29 Januari 2013. Jayadi mengatakan, bahwa hacker yang bernama Wildan tersebut diamankan petugas di sebuah warnet yang terletak di Jember. “Ia merupakan pengelola warnet tersebut.” ujarnya. CITRA I STMIK AMIKOM. 2012, *Seminar Cyber and Drug Crime*. Yogyakarta.
  - 4 Naisbitt and Aburdene (1982), *Megatrends reported that we are shifting from an Industrial Society to an Information Society. Altogether, they proposed ten Megatrends (changes), that would shape the information age:*
    - a. *Industrial Society to Information Society*
    - b. *Forced Technology to High Tech/High Touch*
    - c. *National Economy to World Economy*
    - d. *Short Term to Long Term*
    - e. *Centralization to Decentralization*
    - f. *Institutional Help to Self-Help*
    - g. *Representative Democracy to Participatory Democracy*
    - h. *Hierarchies to Networking*
    - i. *North to South*
    - j. *Either/Or to Multiple Option*

*In one of the trend listed above, “from hierarchies to networking,” an entirely different way of managing information and distributing power was predicted. Various networks would radically transform and increase public access to goods, services, data, on a global scale. This network became today’s Internet. However, with this network came a major drawback...*

kegiatan masyarakat industri. Panitia Kerja Perlindungan Data Dewan Eropa (*The Data Protection Working Party of Europe Council*) menyatakan pula bahwa cybercrimes adalah bagian sisi paling buruk dari masyarakat informasi yang perlu ditanggulangi dalam waktu singkat. Konperensi Cybercrimes International di London, Februari 2001 menyatakan dengan tegas bahwa cybercrime adalah salah satu dari aktivitas kriminal yang paling cepat tumbuh di planet bumi ini. Kerugian yang ditimbulkan luar biasa besarnya yang mencapai US \$ 40 miliar per tahun. Di Amerika Serikat menurut hasil penelitian dari *United States of Computer Security Institute (USCSI)* menunjukkan bahwa sekitar 90% perusahaan (corporates) berskala besar mengaku telah mendeteksi adanya pelanggaran keamanan terhadap sistem komputerisasi yang mereka gunakan dalam kegiatan industri. Sebanyak 273 perusahaan di sana telah mengalami financial losses yang cukup signifikan untuk tambahan modal bagi perkembangan perusahaan tersebut. Nilai kerugian mencapai US \$ 265 juta dan sebagian besar dari transaksi ilegal.<sup>5</sup>

Pada Kongres PBB ke-X tahun 2000, pengertian atau definisi dari cybercrime dibagi dua, yaitu pengertian sempit, yakni ***“any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them”***. Artinya, kejahatan ini merupakan perbuatan bertentangan dengan hukum yang langsung berkaitan dengan sarana elektronik dengan sasaran pada proses data dan sistem keamanan komputer. Di dalam pengertian luas, cybercrime didefinisikan sebagai ***“any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network”***. Artinya, perbuatan yang melawan hukum dengan menggunakan sarana atau berkaitan dengan sistem atau jaringan komputer termasuk kejahatan memiliki secara ilegal, menawarkan atau mendistribusikan informasi melalui sarana sistem atau jaringan komputer. Selain itu, *Cybercrime* dapat juga diartikan sebagai *“crime related to technology,*

*computers, and the internet”*. Artinya, kejahatan yang berkaitan dengan teknologi, komputer dan internet.

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui orang lain maka dapat merugikan korban baik secara materiil maupun immateriil.

Pada perkembangannya dalam cyber crime sendiri kemudian menimbulkan istilah-istilah baru bagi para pelakunya. Mereka yang suka “memainkan” internet, menjelajah ke situs internet orang lain disebut “Hecker” dan perbuatannya disebut “Hacking”. Apabila si hecker yang penyusup dan penyeludup ke situs orang lain itu dan merusak disebut sebagai “Cracker”. “Hacker” yang menjelajah berbagai situs dan “mengintip” data, tetapi tidak merusak sistem komputer, situs-situs orang atau lembaga lain disebut “Hektivism”. Akhir-akhir ini dapat dikatakan motivasi uang yang paling menonjol, yaitu dengan menggunakan data kartu kredit orang lain untuk belanja lewat internet. Cara mereka disebut “carder” beroleh data kartu kredit adalah dengan menadah data dari transaksi konvensional, misalnya pembayaran di hotel, biro wisata, restoran, toko dan lain-lain.

Kendati kejahatan ini kerap terjadi namun hingga sekarang belum ada pilar hukum paling ampuh untuk menangani kasus-kasusnya, bahkan perkembangan kejahatan di dunia cyber semakin dahsyat. Selain menggunakan piranti canggih, modus kejahatan cyber juga tergolong rapi. Begitu hebatnya kejahatan ini bahkan dapat meresahkan dunia internasional. Dinamika cybercrime memang cukup rumit. Sebab, tidak mengenal batas negara dan wilayah. Selain itu, waktu kejahatannya pun sulit ditentukan.

## B. Pembahasan

### 1. Pengertian Hacker

**Peretas** (Inggris: **hacker**)<sup>6</sup> adalah orang yang mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi

5 <http://rizkacil.wordpress.com/2012/06/03/ipitek-serta-perkembangannya/>  
<http://yudhi-hasyim.blogspot.com/2008/11/cyber-crime-dan-upaya-antisipasi.html>

6 <http://id.wikipedia.org/wiki/Peretas>

oleh tantangan.

Terminologi peretas muncul pada awal tahun 1960-an di antara para anggota organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka berkuat dengan sejumlah komputer *mainframe*. Kata bahasa Inggris "hacker" pertama kalinya muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik daripada yang telah dirancang bersama.<sup>7</sup>

Kemudian pada perkembangan selanjutnya muncul kelompok lain yang menyebut-nyebut diri sebagai peretas, padahal bukan. Mereka ini (terutama para pria dewasa) yang mendapat kepuasan lewat membobol komputer dan mengakali telepon (*phreaking*).<sup>8</sup> Peretas sejati menyebut orang-orang ini *cracker* dan tidak suka bergaul dengan mereka. Peretas sejati memandang *cracker* sebagai orang malas, tidak bertanggung jawab, dan tidak terlalu cerdas. Peretas sejati tidak setuju jika dikatakan bahwa dengan menerobos keamanan seseorang telah menjadi peretas.<sup>9</sup>

Para peretas mengadakan pertemuan tahunan, yaitu setiap pertengahan bulan Juli di Las Vegas. Ajang pertemuan peretas terbesar di dunia tersebut dinamakan *Def Con*. Acara Def Con tersebut lebih kepada ajang pertukaran informasi dan teknologi yang berkaitan dengan aktivitas peretasan.

## 2. Hacker dalam Hukum di Indonesia

Istilah teknologi informasi sendiri pada dasarnya merupakan gabungan dua istilah dasar yaitu teknologi dan informasi. Teknologi dapat diartikan sebagai pelaksanaan ilmu, sinonim dengan ilmu terapan. Sedangkan pengertian informasi menurut Oxford English Dictionary,<sup>10</sup> adalah "that of which one is apprised or told: intelligence, news". Kamus lain menyatakan bahwa informasi adalah sesuatu yang dapat diketahui. Namun ada pula yang menekankan informasi

sebagai transfer pengetahuan. Selain itu istilah teknologi informasi juga memiliki arti yang lain sebagaimana diartikan oleh RUU teknologi informasi yang mengartikannya sebagai suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memanipulasi, mengumumkan, menganalisa, dan menyebarkan informasi dengan tujuan tertentu (Pasal 1 angka 1). Sedangkan informasi sendiri mencakup data, teks, image, suara, kode, program komputer, databases (Pasal 1 angka 2).

Karena kurangnya pengetahuan sebagian besar masyarakat kita akan manfaat internet, yang terjadi justru bukan pemanfaatan internet sebagai sarana informing ataupun reforming melainkan hanya sebatas menggunakannya sebagai sarana hiburan. Sehingga internet bukan lagi menjadi sebuah enlightening technology tetapi justru dianggap sebagai penyebab turunnya moral bangsa, sebagai bukti dapat kita lihat dengan maraknya bisnis 'gelap' melalui internet. Sedangkan bagi sebagian computer intellectual internet justru disalahgunakan sebagai sarana untuk memperoleh keuntungan yang menyebabkan kerugian bagi orang lain yang terkenal dengan istilah cyber crime. Untuk itu memang masih diperlukan berbagai upaya untuk dapat mencapai tahapan industri internet yang matang (the Mature Market).

Paling tidak ada dua macam upaya mendasar yang perlu dilakukan yaitu yang pertama melakukan edukasi pasar yang cenderung dilakukan masyarakat internet itu sendiri. Pendidikan ini mencakup pemahaman terhadap teknologi dan macam pelayanan yang diberikan sampai dengan dengan pengetahuan menjadi trouble shooter. Yang kedua adalah mengupayakan biaya rendah dan kemudahan serta keragaman mendapatkan pelayanan bagi setiap pemakai internet, mulai dari pengadaan infrastruktur sampai dengan yang berkaitan dengan software dan hardware. Sehingga apabila hal ini bisa dicapai maka diharapkan bangsa Indonesia akan lebih siap lagi dalam menghadapi era persaingan bebas dan globalisasi.

Perspektif dan Konsep Mengenai Kejahatan Mayantara (Cyber crime). Dalam perkembangannya ternyata penggunaan internet tersebut membawa

<sup>7</sup> Ibid

<sup>8</sup> Ibid

<sup>9</sup> Ibid

<sup>10</sup> Oxford Dictionary



sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti sosial dan perilaku kejahatan sebagai aplikasi dari perkembangan internet, yang sering disebut cyber crime. Dalam dokumen A/CONF.187/1013, "Cyber Crime dalam arti sempit" ("in a narrow sense") disebut "computer crime" dan "Cyber Crime dalam arti luas" ("in a Broader sense") disebut computer related crime (CRC). Walaupun jenis kejahatan ini belum terlalu banyak diketahui secara umum, namun The Federal Bureau of Investigation (FBI) dalam laporannya mengatakan bahwa tindak kejahatan yang dapat dikategorikan cyber crime telah meningkat empat kali lipat sejak tiga tahun belakangan ini<sup>14</sup>, dimana pada tahun 1998 saja telah tercatat lebih dari 480 kasus cyber crime di Amerika Serikat. Hal ini telah menimbulkan kecemasan lebih dari 2/3 warga Amerika Serikat.

Cyber crime sendiri memiliki berbagai macam interpretasi. Sering diidentikkan dengan computer crime. The U.S. Department of Justice memberikan pengertian computer crime sebagai: "...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution". Computer crime pun dapat diartikan sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Dari beberapa pengertian di atas, computer crime dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai obyek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas computer crime didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi yang canggih<sup>16</sup>. Ada kontradiksi yang sangat mencolok untuk menindak kejahatan seperti ini. Dalam hukum diperlukan adanya kepastian termasuk mengenai alat bukti kejahatan, tempat kejahatan dan korban dari tindak kejahatan tersebut, sedangkan dalam computer crime ini semuanya serba maya, lintas negara dan lintas waktu.

Meskipun begitu ada upaya untuk memperluas pengertian komputer agar dapat melingkupi segala kejahatan di internet dengan peralatan apapun, seperti pengertian computer dalam The Proposed West Virginia Computer Crime Act, yaitu: "an electronic, magnetic, optical, electrochemical,<sup>11</sup>

atau:

#### 1) *Cyber Sabotage and Extortion.*

Kejahatan ini dilakukan dengan membuat gangguan, pengrusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan sebagaimana mestinya, atau berjalan sebagaimana yang diperintahkan oleh pelaku.

#### 2) *Offense against Intellectual Property*

Kejahatan ini ditujukan terhadap Hak Atas Kekayaan Intelektual yang dimiliki pihak lain di internet.

#### 3) *Infringements of Privacy*

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui orang lain maka dapat merugikan korban baik secara materiil maupun immateriil.

Hukum, di Indonesia masih banyak yang belum disesuaikan dengan perkembangan iptek, terutama yang berkaitan dengan tindak pidana. Harus diakui bahwa Indonesia belum mengadakan langkah-langkah yang cukup signifikan di bidang penegakan hukum (*law enforcement*) dalam upaya mengantisipasi kejahatan mayantara seperti dilakukan oleh negara-negara maju di Eropa dan Amerika Serikat. Kesulitan yang dialami adalah pada perangkat hukum atau undang-undang teknologi informasi dan telematika yang belum ada sehingga pihak kepolisian Indonesia masih ragu-ragu dalam bertindak untuk menangkap para pelakunya, kecuali kejahatan mayantara yang bermotif pada kejahatan ekonomi/perbankan.

Hasil Seminar Hukum Nasional VIII di Bali, 31 Mar 2003<sup>12</sup> yang bertema "**Penegakan Hukum Dalam Era Pembangunan Nasional Berkelanjutan**" disusun Rekomendasi Grand Design dalam Perencanaan dan Legislasi Nasional,

<sup>11</sup> Sumber: <http://www.ketok.com/forum/viewtopic.php?t=215>

<sup>12</sup> Barda Nawawi Arief, 2010, *Hasil Seminar Hukum Nasional VIII di Bali, 31 Mar 2003*. Semarang, Pustaka Magister

sebagai berikut :

- a. Proses perencanaan dan legislasi nasional dilakukan melalui penelitian dan pengkajian secara mendalam yang meliputi aspek asas-asas, norma, institusi dan seluruh prosesnya yang dituangkan dalam suatu Naskah Akademik peraturan perundang-undangan. Naskah Akademik itu sendiri merupakan landasan dan pertanggungjawaban akademik untuk setiap asas dan norma yang dituangkan dalam rancangan undang-undang.
- b. Penyusunan legislasi harus harmonis secara horisontal dan tidak bertentangan dengan ketentuan yang lebih tinggi secara vertikal. Ketidakkonsistenan terhadap dua unsur tersebut akan berakibat timbulnya biaya tinggi, ketidakpastian hukum, dan konflik kewenangan antar institusi hukum.
- c. Naskah akademik dan RUU yang harus dibuat melalui suatu penelitian dengan memperhatikan nilai-nilai ilmiah normatif dan praktik yang terjadi dan secara konsisten memperhatikan dan mendasarkan pada hierarki peraturan perundang-undangan. Oleh karenanya produk hukum harus sesuai dan konsisten dengan kaidah yang ada di dalam UUD 1945. Konsistensi semacam ini akan secara optimal memberikan maslahat bagi bangsa dan negara. Dengan kata lain, aspek filosofis, aspek yuridis dan aspek sosiologis yang disertai keajegan pada landasan filosofis dan konstitusi harus selalu diperhatikan secara cermat dalam pembuatan peraturan perundang-undangan.
- d. Proses harmonisasi harus dimulai dari Naskah akademik, salah satu yang harus dimuat dalam naskah akademik adalah adanya pembahasan komparatif RUU yang akan dibuat dan keterkaitannya dengan hukum positif yang ada. Dengan demikian diperlukan adanya suatu regulasi yang mengatur tatacara dan proses pembahasan Naskah Akademik dalam rangka Program Legislasi Nasional.
- e. Pembangunan hukum tidaklah terlepas dari sejarah, karena itu dengan telah dimulainya reformasi tidaklah berarti kita memulai segala sesuatunya dari nol. Semua hal yang baik yang ada dalam produk-produk hukum positif yang sudah ada harus menjadi modal pembangunan

hukum, sementara yang tidak baik dan tidak sesuai lagi harus kita koreksi dan perbaiki. Pembangunan hukum adalah konsep yang berkesinambungan dan tidak pernah berhenti sehingga masalah keadilan, penegakan hukum dan sikap masyarakat terhadap hukum tidak boleh mengabaikan keadaan dan dimensi waktu saat hukum itu ditetapkan/berlaku. Selain tidak bijaksana, hal tersebut pada gilirannya juga akan berpotensi mengingkari asas dan kepastian hukum itu sendiri. Menafsirkan hukum dengan metode historis selain metode penafsiran lainnya seperti gramatikal dan sistematis adalah penting untuk dilakukan untuk memahami 'roh' hukum yang sesungguhnya.

- f. Legislasi yang dilaksanakan dengan baik dapat menjadikan hukum berfungsi menjadi pemberi arah bagi masyarakat untuk menjadi masyarakat yang baik.

Dari Rekomendasi dalam Seminar Hukum diatas, di Indonesia mulai disusun pembaharuan hukum yang mengarah pada penyesuaian lptek dan situasi Global, diantaranya dengan mengkriminalisasikan kegiatan di *cyberspace* dengan pendekatan global. Selain melakukan upaya dengan mengkriminalisasikan kegiatan di *cyberspace* dengan pendekatan global, Pemerintah Indonesia sedang melakukan suatu pendekatan *evolusioner* untuk mengatur kegiatan-kegiatan santun di *cyberspace* dengan memperluas pengertian-pengertian (ekstensif interpretasi) yang terdapat dalam Konsep KUHP Baru. Artinya, Konsep KUHP Baru sebelumnya tidak memperluas pengertian-pengertian yang terkait dengan kegiatan di *cyberspace* sebagai delik baru.

Menurut Barda Nawawi Arief,<sup>13</sup> kebijakan yang ditempuh dalam Konsep KUHP Baru yang berkaitan dengan kegiatan *cyberspace* antara lain: (1) dalam Buku I (ketentuan umum) dibuat ketentuan mengenai (a) pengertian "barang" (Pasal 174) yang di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon atau telekomunikasi atas jasa komputer. (b) pengertian "anak kunci" (Pasal 178) yang di dalamnya termasuk kode rahasia, kunci masuk komputer, kartu magnetik, sinyal yang telah diprogram untuk membuka sesuatu. (c) pengertian "surat" (Pasal 188) termasuk data tertulis atau

13 Barda Nawawi Arief, 2006, *Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia*. PT Gafindo Persada hlm. 2

tersimpan dalam disket, pita magnetik, media penyimpanan komputer atau penyimpanan data elektronik lainnya. (d) pengertian "**ruang**" (Pasal 189) termasuk bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu oleh pelaku. (e) pengertian "**masuk**" (Pasal 190) termasuk mengakses komputer atau masuk ke dalam sistem komputer. (f) pengertian "**jaringan telepon**" (Pasal 191) termasuk jaringan komputer atau sistem komunikasi komputer. (2) dalam Buku II memuat delik-delik baru yang berkaitan dengan kemajuan teknologi dengan harapan dapat menjaring kasus-kasus *cybercrime* antara lain (a) menyadap pembicaraan di ruangan tertutup dengan alat bantu teknis (Pasal 263), (b) memasang alat bantu teknis untuk tujuan mendengar atau merekam pembicaraan (Pasal 264), (c) merekam (memiliki) atau menyiarkan gambar dengan alat bantu teknis di ruangan tidak untuk umum (Pasal 266), (d) merusak atau membuat tidak dapat dipakai bangunan untuk sarana atau prasarana pelayanan umum, seperti bangunan telekomunikasi atau komunikasi lewat satelit atau komunikasi jarak jauh (Pasal 546), dan (e) pencucian uang (Pasal 641–642).

Usaha yang dilakukan di atas adalah melalui regulasi undang-undang dengan menggunakan sarana penal, yakni memperluas pengaturan *cyberspace* dalam Konsep KUHP Baru dan membuat suatu RUU Teknologi Informasi dan RUU Telematika yang berkaitan dengan kegiatan di *cyberspace*. Akan tetapi yang perlu diperhatikan adalah pengkajian lebih intensif terhadap masalah yang hendak dikriminalisasikan sebagai upaya penanggulangan kejahatan mayantara. Persyaratan pokok adalah kerugian korban yang signifikan dengan perbuatan pelaku. Ketentuan pidana harus dapat dioperasionalkan dan keyakinan bahwa tidak ada sarana lain yang betul-betul dapat mengatasinya.

### C. Simpulan

Pada perkembangannya dalam cyber crime sendiri kemudian menimbulkan istilah-istilah baru bagi para pelakunya. Mereka yang suka "memainkan" internet, menjelajah ke situs internet orang lain disebut "Hecker" dan perbuatannya disebut "Hacking". Apabila si hecker yang penyusup dan penyeludup ke situs orang lain itu dan merusak disebut sebagai "Cracker". "Hecker" yang

menjelajah berbagai situs dan "mengintip" data, tetapi tidak merusak sistem komputer, situs-situs orang atau lembaga lain disebut "Hektivism". Akhir-akhir ini dapat dikatakan motivasi uang yang paling menonjol, yaitu dengan menggunakan data kartu kredit orang lain untuk belanja lewat internet. Cara mereka disebut "carder" beroleh data kartu kredit adalah dengan menadah data dari transaksi konvensional, misalnya pembayaran di hotel, biro wisata, restoran, toko dan lain-lain.

Kendati kejahatan ini kerap terjadi namun hingga sekarang belum ada pilar hukum paling ampuh untuk menangani kasus-kasusnya, bahkan perkembangan kejahatan di dunia cyber semakin dahsyat. Selain menggunakan piranti canggih, modus kejahatan cyber juga tergolong rapi. Begitu hebatnya kejahatan ini bahkan dapat meresahkan dunia internasional. Dinamika cybercrime memang cukup rumit. Sebab, tidak mengenal batas negara dan wilayah. Selain itu, waktu kejahatannya pun sulit ditentukan. Lengkap sudah fenomena Cyber Crime untuk menduduki peringkat calon kejahatan terbesar di masa mendatang.

### DAFTAR PUSTAKA

- Arief, Barda Nawawi, 2006, *Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia*. PT Gafindo Persada
- Arief, Barda Nawawi, dalam "Kebijakan Kriminalisasi dan Masalah Yurisdiksi Tindak Pidana Mayantara", Seminar Nasional RUU Teknologi Informasi (Cyber-Law) "Pemberdayaan Teknologi Informasi dalam Masyarakat Informasi", Kerjasama Dirjen Postel DEPHUB dengan UNDIP, Gedung Ghradhika Bhakti Praja, Semarang, 26 Juli 2001.
- Arief, Barda Nawawi, 2011. *Pornografi, Cyberporn dan Porno Aksi*, Semarang: Badan Penerbit Universitas Diponegoro
- Arief, Barda Nawawi, 2010, *Hasil Seminar Hukum Nasional VIII di Bali, 31 Mar 2003*, Semarang: Pustaka Magister
- Naisbitt and Aburdene *Megatrends* (1982). Anonim. CITRA I STMIK AMIKOM. *Seminar Cyber and Drug Crime*. Yogyakarta. 2012
- <http://id.wikipedia.org/wiki/Peretas>

<http://rizkacil.wordpress.com/2012/06/03/iptek-serta-perkembangannya/>  
<http://www.ketok.com/forum/viewtopic.php?t=215>  
<http://yudhi-hasyim.blogspot.com/2008/11/cyber-crime-dan-upaya-antisipasinya.html>